Manual Part and Parent Policy: Information Services (IS) Information Security Policy	Procedure Number: IS9-1PR	Alberta Policing Standards: OP 6.1, OP 6.4, OP 6.5, SS 8.8

Security Classification of Information Procedure

Purpose:

The EPS information security classification scheme has been developed for the purpose of ensuring that personal and/or confidential information is adequately protected from unauthorized access, use, or disclosure, and to ensure that information shared between law enforcement, municipal, provincial, and federal government agencies is handled according to common classification principles.

The application of a security classification to a record does not affect the rules for the collection, use, or disclosure of information as set out in the *Access to Information Act (ATIA)*.

Definitions:

Definitions listed in this section apply to this document only with no implied or intended organization-wide or EPS Policy and Procedure Manual wide use.

Information – Operational and administrative records, intelligence, knowledge or data, regardless of how it is stored, kept or shared. It includes electronic data, written or printed information and verbal conversation.

Procedure:

A. Applying the Information Security Classification Scheme:

All EPS information must be classified in accordance with the following levels and descriptors:

1. Unclassified:

   The Unclassified classification is applied to public information including information deemed public by legislation or through a policy of routine disclosure.

   a. Examples of Unclassified Information:

      Media releases, job postings, public hearing/meeting notices, information or reports intended for the public via the EPS or related websites, etc.

b. Access to Unclassified Information:

Available to the public, all employees, contractors, sub-contractors, and agents.

c. Marking of Unclassified Information:

None.

d. Protective Measures:

See **IS10-1PR Information Technology Use and Management Procedure**.

2. Protected A:

The Protected A classification is applied to information that is sensitive outside the EPS. The disclosure of such information could reasonably be expected to cause harm to the EPS by revealing operational, tactical, investigative, or business information, or the personal information of employees or citizens.

a. Examples of Protected A Information:

General or routine case files, arrest reports, Crown disclosure, daily operational highlights, general business e-mail, EPS Policy and Procedure manual, etc.

b. Access to Protected A Information:

Authorized access to employees, contractors, sub-contractors, and agents on a "need-to-know" basis for business-related purposes.

c. Marking of Protected A Information:

None / Optional. Any member of the EPS is authorized to mark a document as Protected “A”. All intelligence documents should be marked with the appropriate protection level if disseminated outside of the EPS.

d. Protective Measures:

i. See **IS10-1PR Information Technology Use and Management Procedure**, and

ii. do not leave in public areas.

e. Examples of Protected A Information Systems and Environments:

i. the CAD dispatch system,

ii. the HEAT Help Desk system, and

iii. unencrypted e-mail.

3. Protected B:

The Protected B classification is applied to information that is intended for police use only. The disclosure of such information could reasonably be expected to cause significant harm to the EPS' operations, public loss of confidence in the EPS, damage to partnerships, relationships, or reputation, or may result in a serious privacy breach. Mere 'confidentiality' is not of itself grounds for classifying information above Protected A.

a. Examples of Protected B Information:

Intelligence reports, Professional Standards Branch files, Crime Stoppers tips, EPS personnel files, medical records, policy and operational plans not yet implemented, records subject to legal privilege, Threat / Risk Assessments / Memorandums from Organizational Security Section, etc.

b. Access to Protected B Information:

Access is restricted to police use only.

c. Marking of Protected B Information:

When disclosed outside of the EPS the document or file is to be marked 'Protected B'. For intelligence reports protection level should be marked even for distribution within the EPS. Any member of the EPS is authorized to mark a document as Protected "B," however Protected B classifications may be subject to review and change by the member i/c the CAD and NICHE Management and Development Unit.

d. Protective Measures:

i. See **IS10-1PR Information Technology Use and Management Procedure**,

ii. all protective measures listed for Protected A information (A.2.d),

iii. protected B information will be encrypted if sent by e-mail externally (for example, by using the 'Encrypt Message" feature in Outlook e-mail or an encrypted zip file),

iv. will not be disclosed to the public without authorization from the author, the staff sergeant i/c the relevant Section or Branch, or by members of Information and Privacy Unit (IAPU) or Legal Advisors Section,

v. printed documents will be stored in a physically secure manner (controlled office, locked drawer or cabinet),

vi. hard copies will be shredded when destruction or disposal is required, and

vii. local storage of Protected B information should be limited and must only occur on specifically authorized devices or in specifically authorized internet based storage environments.

e. Examples of Protected B Information Systems and Environments:

i. the NicheUA records management system,

ii. the IAPro records management system, and

iii. the IAPU and Legal Advisors operational areas.

4. Protected C:

The Protected C classification is applied to information that is highly sensitive. The disclosure of such information could cause loss of life, risks to public safety, substantial financial loss, social hardship, and/or major economic impact.

a. Examples of Protected C Information:

Information identifying confidential human sources and/or agents, undercover operators, surveillance or covert law enforcement operations, risk assessments, etc.

b. Access to Protected C Information:

Authorized access available only to specific individuals, units or operational areas.

c. Marking of Protected C Information:

When disclosed outside of its originating area of EPS the document or file must be clearly marked ‘Protected C’. Protected C classification requires the approval of the inspector i/c the area it applies to, or the duty officer, if after hours approval is necessary.

d. Protective Measures:

i. See **IS10-1PR Information Technology Use and Management Procedure**,

ii. all protective measures listed for Protected A and Protected B information (A.2.d, A.3.d),

iii. information must NOT be stored in NicheUA or any other system that is not classified for Protected C,

iv. information must NOT be sent by e-mail,

v. printed documents must be stored only in physical locations that meet enhanced security standards (including safes and high-security cabinets, lockable offices OFF the master key system with reinforced construction), and

vi. for more specific information on the storage of Protected C information contact Investigative Services Branch.

e. Examples of Protected C Information Systems and Environments:

The Source Management Unit and operational area.

B. Third Party Rule:

1. Any information received from another agency and marked with “Third Party Rule” must not be further disclosed or shared by the EPS without the consent of the originating author or agency.

2. All information received from other agencies MUST be treated in accordance with the protection level assigned by the originating agency and MUST be handled in accordance with the rules and procedures established by that agency or as set out in any applicable MOU.

3. Should the EPS members receiving information not be able to provide the same level of protection required by the originating agency, this should be made clear to the originating agency before the information is collected.

4. The Third Party Rule also applies to all Protected B and C information that is shared with other agencies by the EPS. All such records being disclosed should be marked with “Third Party Rule” and/or with the appropriate protection level in order to avoid inadvertant disclosure of sensitive EPS information to a third party.

5. Questions about information sharing or the disclosure of EPS records should be directed to members of IAPU or Legal Advisors Section. Questions about Crown disclosure should be directed to Court Services Unit.

6. **IS - Appendix C - Corresponding Classification Systems** provides the corresponding classification systems for information received by the EPS from outside agencies.

Review:	Revision Date:	No.:
	2019 December 18	
	2023 June 02	PrR23-003
	2024 October 03	
	2025 July 31	

Related Information:

Policy:	IS10PO Information Technology Use and Management Policy
Procedure:	IS10-1PR Information Technology Use and Management Procedure IS10-2PR Recording and Reporting the Use of IT Resources Procedure
How-To:	E-mail Encryption
Appendices:	IS - Appendix C - Corresponding Classification Systems